Plagiarism Checker X Originality Report

Similarity Found: 22%

Date: Friday, April 05, 2019
Statistics: 426 words Plagiarized / 1980 Total words
Remarks: Medium Plagiarism Detected - Your Document needs Selective Improvement.

International Journal of Engineering & Technology, 7 (3.5) (2018) 131-133 International Journal of Engineering & Technology Website: www.sciencepubco.com/index.php/IJET Research paperr Security Enhancement with USB Flash Disk as Key using AES Algorithm Robbi Rahim1, Solly Aryza2, H Herdianto2, Parma Hadi Rantelinggi3, Agustinus Suradi4, Dwi Ermayanti Susilo5, Perawati Bte Abustang6, Waddi Fatimah6, Eka Fitriana HS6, Beatus Mendelson Laka7, A Arfin8, S Sriwahyuni6, Muh Reski Salemuddin6, A Akhiruddin6 1Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia 2Universitas Pembangunan Panca Budi, Medan, Indonesia 3Universitas Papua, Indonesia 4Faculty of Computer Science, Universitas Widya Dharma, Indonesia 5STIE PGRI Dewantara Jombang, Indonesia 6Sekolah Tinggi Ilmu Keguruan dan Ilmu Pendidikan Mega Rezky, Makassar, Indonesia 7Sekolah Tinggi Keguruan dan Ilmu Pendidikan Biak Papua, Indonesia 8Universitas Muhammadiyah Kendari, Kendari, Indonesia *Corresponding author E-mail: usurobbi85@zoho.com Abstract Current data and information security is very important to do so that there is no abuse by irresponsible parties.

Cryptograph y is one method that can be used to secure data or information and the Advanced Encrryption Standard (AES) algorithm is one of the cryptographic algorithms that can be used. The encryption and decryption process in Cryptography cannot be done without using a key, and the key used in this research is a USB Flash Disk. Tests performed get results that the cryptographic process is better for users because they do not have to remember the keys used but are at risk if the USB Flash Disk used is lost then the data or inform ation cannot be opened again. Keywords: Cryptography, Encryption Decryption, USB Encryption 1.

Introduction

In the current era of globalization, computers are a tool that is needed by many state-owned and private institutions and compa- nies[1]–[3]. Computer usage today is growing rapidly in all fields in accordance with the progress of the times. This is marked by the increasing types of computer operating systems used starting from Microsoft Windows, Mac OS to Linux.

However, there are still rare people who understand how to lock or secure a file so that it cannot be accessed by others. This is due to the complexity of computer security procedures when using the facilities provided by each operating system. For that, it takes an application that can easily and quickly lock and secure the user's computer by using keywords that are entered into it[4], [5].

In order to produce keyword-based computer security that has a high level of confidentiality, it must be encoded with the password for both the locking process and the security unlock process. One encryption method that is good enough to use is the Advanced Encryption Standard (AES) algorithm[6]–[8]. By using the AES algorithm, the keywords will be encrypted first when stored for later decryption during the verification process.

The keywords used are keys from flash disk so that the data security process will be better, for the encryption process decryption of flash disk files must be recognized first if there is no flash disk then the encryp- tion and decryption process cannot be done. The choice of flash disk as an encryption key is also very im- portant and this is the main reason why the author chose to use _flash disk as the encryption key.

Flash disk is used as a key to files that will be encrypted, the use of flash disk will be safer because each flash disk does not have the same serial, without flash disk it is impossible for the file to be encrypted or decrypted. 2. Methodology USB Flash Disk is a hardware that is commonly used to store files on a computer[9], so that the file can be taken anywhere and at any time can be modified.

The use of flash as a key is very appr o- priate because it is like a hardware dongle (USB Dongle) which is commonly used as a password to enter the system such as the magic software and zahir accounting that uses USB Dongle as an access key. USB Flash is of course like other hardware has a unique serial number and will not be the same because it has a different base assembly register even though it has the same IC, it is the use of the flash disk serial number that is accessed to be used as a key so that only the user has the flash disk who can do the encryption and decryption process. Cryptography is the study of how a message or document is safe, cannot be read by unauthorized parties.

In its development, cryp- tography is also used to identify message senders with digital si g- natures and authenticity of messages with digital fingerprints.

In maintaining data confidentiality, cryptography transforms plaintext into a form of ciphertext that cannot be recognized. This ciphertext is then sent by the sender to the receiver. After arriving at the recipient, the ciphertext is transformed back into the plaintext form so that it can be recognized[10]–[14].

In another sense, cryptography is the art and science of securing messages. In the world of cryptography, messages are called plaintext or cleartext. The process of disguising messages in such a way as to hide the original contents is called encryption. An encrypted message is called ciphertext. The AES algorithm uses substitution, permutation and a number _B. Summing bits between plaintext blocks and keys C.

Transforming rounds as many times as Nr with the following results:

of rounds imposed on each block that will be decrypted. For each _02 03 01 01 _63 09 cd ?? _5? 57 ?7 1?

round, AES uses a different key. The key of each round is called a _[01 02 03 01] [53 65 70 ??] = [72 ?5 ?? ?9]

round key.

AES operates in byte orientation so that it is possible to implement efficient algorithms into software and hardware. The block size for the AES algorithm is 128 bits (16 bytes)[15]–[18]. AES supports 128-bit to 256-bit key lengths with 32-bit steps. The key length and block size can be chosen independently. Each _01 01 02 03 03 01 01 02 D.

AddRoundKey 5? 57 ?7 1? _?0 ?1 ?7 ?0 8? 04 51 ?7 ?6 ?2 da ?6 _64 ?? 3? ?9 15 92 29 1? 89 85 2? ??

block is encrypted in a certain number of turns. The AES algo- _[72 ?5 ?? ?9] [?? ?? ?6 ??] = [?8 5? 18 12]

rithm has 3 (three) parameters: a. Plaintext is a 16-byte array containing input data. b. Ciphertext is an array of 16-byte size, which contains the re- _64 ?? 3? ?9 15 92 29 1? _74 72 78 76 ?? ?? ?1 ?? _10 ?? 43 8? ?8 68 ?8 ??

sults of encryption. c.

The key is a 16-byte array, which contains a cipher key (also called a cipher key). An outline of the AES algorithm that operates on 128-bit blocks with 128-bit keys is as follows: a. AddRoundKey, XOR between the initial state (plaintext) and the cipher key. This stage is also called the initial round. b. Round as much as Nr-1 times.

The process carried out in each round is: 1) SubBytes is a substitution of bytes using a substitution ta- ble (S-Box). 2) ShiftRows is a shift in the array array states by wrapping. 3) MixColumns is scrambling data in each array column state. AddRoundKey is XOR between the statesnow round key. c. Final round, the process for the last round: 1) SubBytes 2) ShiftRows 3) AddRoundKey 3.

Results and Discussion For the AES encryption process, the plaintext is transformed re- peatedly for several rounds. The number of round transformations (Nr) depends on the value of Nk and Nb. Nk is the key length divided by 32, while Nb is the length of the block divided by 32. Plaintext: Robbi Rahim Key: 200517415207D7538543 (32 30 30 35 31 37 34 31 35 32 30 37 44 37 35 33 38 35 34 33) A. Key Expansion Table 1.

Roundkey Encryption _For rounds from AES, there are 10 rounds. From the above steps, the ciphertext is obtained as follows: 69c4e0d86a7b0430d8cdb78070b4c55a the decryption process is not much different from encryption, it is just inverse for every process. 4.

Conclusion USB Flash Disk as a key to the security process is very possible and very good to use, one of the factors is that the serial number on the USB Flash Disk will not be the same and will not be possible to duplicate, but also if the USb Flash Disk is lost then the decryption process cannot done and this is one of the disadvantages of using a USB Flash Disk as a key. Future development of the weaknesses of using USB Flash Disk as a key can be handled better. References [1] A.

Putera, U. Siahaan, and R. Rahim, “Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm,” Int. J. Secur. Its Appl., vol. 10, no. 8, pp. 173–180, Aug. 2016. [2] R. Rahim, “Man-in-the-middle-attack prevention using interlock protocol method,” ARPN J. Eng. Appl. Sci., vol. 12, no. 22, pp. 6483–6487, 2017. [3] M. Mesran, M. Syahrizal, and R. Rahim, “Enhanced Security for Data Transaction with Public Key Schnorr Authentication and Digital Signature Protocol,” ARPN J. Eng.

Appl. Sci., vol. 13, no. 11, pp. 3839–3846, 2018. [4] R. Nasution, Surya Darma; Ginting, Guidio Leonarde; Syahrizal, Muhamad; Rahim, S. D. Nasution, G. L. Ginting, M. Syahrizal,

and R. Rahim, “Data Security Using Vigenere Cipher and Goldbach Codes Algorithm,” Int. J. Eng. Res. Technol., vol. 6, no. 01, pp. 360–363, 2017. [5] R. Rahim, “APPLIED POHLIG-HELLMAN ALGORITHM IN THREE-PASS,” J. Appl. Eng. Sci., vol. 16, no. 3, pp. 424–429, 2018. [6] D. Chandravathi and P.

V. Lakshmi, “Advanced Homomorphic Encryption for Cloud Data Security,” JOIV Int. J. Informatics Vis., vol. 1, no. 4, p. 1, Mar. 2017. [7] A. Widarma, “Kombinasi Algoritma AES, RC4, dan Elgamal dalam Skema Hybrid untuk Keamanan Data,” J. Comput. Eng. Syst. Sci., vol. 1, no. 1, pp. 1–8, 2016. [8] H. Tange and B.

Andersen, “Attacks and countermeasures on AES and ECC,” in 16th International Symposium on Wireless Personal Multimedia Communications (WPMC), 2013, pp. 1–5. [9] J. Arvin S. Lat, R. Xavier R. Bondoc, and K. C. V. Atienza, “SOUL System: secure online USB login system,” Inf. Manag. Comput. Secur., vol. 21, no. 2, pp. 102–109, 2013.

[10] H. Nurdiyanto et al., "Authentication Security in Radio Frequency Identification with IDEA Algorithm," IOP Conf. Ser. Mater. Sci. Eng., vol.

384, p. 012042, Jul. 2018. [11] D. Abdullah et al., "Super-Encryption Cryptography with IDEA and WAKE Algorithm," J. Phys. Conf. Ser., vol. 1019, no. 1, p. 012039, Jun. 2018. [12] H. Nurdiyanto, R. Rahim, A. S. Ahmar, M. Syahril, M. Dahria, and H. Ahmad, "Secure a Transaction Activity with Base64 Algorithm and Word Auto Key Encryption Algorithm," J. Phys. Conf. Ser., vol. 1028, no. 1, p. 012053, Jun. 2018.

[13] M. Mesran et al., "Combination Base64 and Hashing Variable Length for Securing Data," J. Phys. Conf. Ser., vol. 1028, p. 012056, Jun. 2018. [14] H. Nurdiyanto and R. Rahim, "Enhanced pixel value differencing steganography with government standard algorithm," in 2017 3rd International Conference on Science in Information Technology (ICSITech), 2017, pp. 366–371. [15] G. Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," Int. J. Comput. Appl.,

vol. 6, no. 19, pp. 33–38, 2013. [16] R. Ratnadewi, R. P. Adhie, Y. Hutama, J. Christian, and D. Wijaya, "Implementation and performance analysis of AES-128 cryptography method in an NFC-based communication system," World Trans. Eng. Technol. Educ., vol. 15, no. 2, pp. 178–183, 2017. [17] H. Delfs and H. Knebl, Information Security and Cryptography, vol. 19. 2007. [18] R. A. Mollin, An introduction to cryptography.

Chapman & Hall/CRC, 2007.

INTERNET SOURCES:

<1% -
https://support.symantec.com/content/unifiedweb/en_US/article.TECH148865.html
<1% - https://www.educba.com/cryptography-vs-encryption/
1% - https://file.scirp.org/pdf/AJIBM_2013122310152129.pdf
1% -
https://www.cambridge.org/core/services/aop-cambridge-core/content/view/F2C597292793A3785BB87FFAD484DF0D/S0022112017005377a.pdf/effect_of_a_surface_tension_imbalance_on_a_partly_submerged_cylinder.pdf
1% -
https://www.academia.edu/10395418/A_Cryptosystem_for_Encryption_and_Decryption_of_Long_Confidential_Messages
<1% -
https://www.researchgate.net/publication/2383441_Hiding_The_Hidden_A_Software_System_For_Concealing_Ciphertext_As_Innocuous_Text
1% - https://www.ripublication.com/ijaer17/ijaerv12n23_76.pdf
<1% - http://www.digitalxplore.org/up_proc/pdf/47-139341474267-71.pdf
<1% - http://ww1.microchip.com/downloads/en/AppNotes/00953a.pdf
<1% - http://airccse.org/journal/IS/papers/2612ijist01.pdf
<1% - https://en.wikipedia.org/wiki/Transport_Layer_Security
<1% -
https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.2.0/com.ibm.zos.v2r2.csfb400/ktb.htm
1% - http://ijsrst.com/paper/4857.pdf
1% -
https://www.academia.edu/363232/DESIGN_OF_AUDIO_DIGITAL_WATERMARKING_FOR_SONGS_COPYRIGHT_AUTHENTICATION_APPLICATION_USING_RIJNDAEL_ENCRYPTION
<1% - http://ijns.femto.com.tw/paper_upload/IJNS-2007-05-29-1-r.doc
1% -
https://media.hotnews.ro/media_server1/document-2012-05-10-12218184-0-ic11-mang-erica-2-2.pdf
<1% - http://ethesis.nitrkl.ac.in/310/1/final_thesis_modified.pdf
<1% -
https://www.academia.edu/31220783/Cryptography_Technique_with_Modular_Multiplication_Block_Cipher_and_Playfair_Cipher
<1% - https://www.minitool.com/data-recovery/usb-flash-drive-not-recognized.html
<1% -
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831507(v=ws.11)
1% -
https://www.researchgate.net/publication/326634777_Entrepreneurship_Intention_Predi

ction_using_Decision_Tree_and_Support_Vector_Machine
1% - https://qiita.com/kaizen_nagoya/items/d6db5de2628a8ebfed94
1% -
https://www.researchgate.net/publication/328003649_Web_based_testing_application_security_system_using_semantic_comparison_method
1% -
https://ijaers.com/detail/an-improved-aes-cryptosystem-based-genetic-method-on-s-box-with-256-key-sizes-and-14-rounds/
1% -
https://www.researchgate.net/publication/327390052_Application_of_Data_Encryption_Standard_and_Lempel-Ziv-Welch_Algorithm_for_File_Security
1% -
https://www.researchgate.net/publication/327550727_Application_of_Invisible_Image_Watermarking
1% -
https://www.researchgate.net/publication/326990164_Prototype_file_transfer_protocol_application_for_LAN_and_Wi-Fi_communication
<1% - http://iopscience.iop.org/issue/1742-6596/1028/1
1% - http://jeneza.com/download_5c734153097c47f56f8b456f.html
1% -
https://www.researchgate.net/publication/326346256_Increase_the_PSNR_of_image_using_LZW_and_AES_algorithm_with_MLSB_on_steganography
<1% - http://www.cayrel.net/?Code-based-cryptography-133